FPKIMA Newsletter

Fall 2014
Volume 1 Issue 2

Federal PKI Management Authority
Enabling Trust

INSIDE THIS ISSUE

Did you know....

The Home Depot and Target breaches were initiated through social engineering and weak authentication? To protect your account and information, do not click on links from suspicious emails and use strong authentication such as your CAC/PIV card when logging into your computer.

Federal Public Key Infrastructure

Federal Common Policy Certification Authority

The Federal Public Key Infrastructure (FPKI) was created in the year 2000 to help ensure electronic services such as physical and logical access, information sharing, and electronic document signing (to name a few) are both secure and trusted. The FPKI facilitates those services between Federal agencies, universities, state governments, commercial entities, international partners, and other communities of interest. The FPKI Management Authority (FPKIMA) operates the FPKI Trust Infrastructure which consists of the hardware and software that run the FPKI's four Certification Authorities (CA). The FPKI CAs include the Federal Bridge (FBCA), Federal Common Policy (FCPCA), E-Governance (EGCA), and the SHA1 Federal Root (SHA1FRCA). This second in a series of four articles will focus on the FCPCA and give a brief description of its history and operation.

The FCPCA was created after the FBCA with the goal of lessening the burden on individual agencies operating and managing a PKI under a common Federal Certificate Policy. This was accomplished by establishing a Shared Service Provider (SSP) Program to facilitate outsourcing of PKI services. The SSPs are certified in a hierarchical PKI model under the FCPCA, which is the trust anchor for the Federal Government, according to the Federal Identity, Credential, and Access Management (FICAM) Roadmap. The FCPCA certifies all CAs issuing PIV certificates either directly or through the FBCA. This operational model differs from the FBCA where Affiliate CAs are connected in a non-hierarchical or bridge model, allowing Affiliate CAs to issue certificates to each other and letting organizations choose which root certificate to use as a trust anchor.

To provide trust services, the FPKI uses a set of policies and procedures based on Public Key Cryptography. The policies and procedures are documented in a Certificate Policy (CP) that defines the requirements and policies for certificate issuance and a Certification Practice Statement (CPS) that documents the internal practices and procedures for certificate lifecycle services. Under the FCPCA, the SSP writes a CPS that corresponds with the Common Policy CP and issues certificates that assert the certificate policies defined in the Common Policy CP. This is unlike the FBCA CP where each cross-certified Affiliate's CP is mapped to the FBCA CP, but has a CPS corresponding to the Affiliate's CP and issues certificates that assert certificate policies specific to the Affiliate's CP.

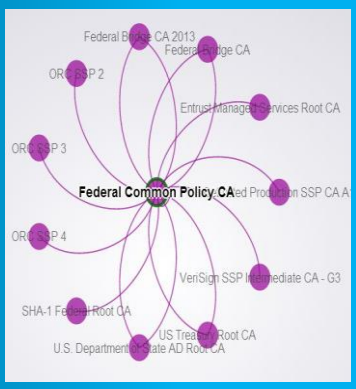
The FCPCA is cross-certified with the FBCA, making it, and the SSP CAs, technically interoperable with the FBCA and all other cross-certified PKIs. This interoperability allows Affiliates with no direct relationship to the FCPCA to trust digital certificates issued by any Affiliate of the FPKI whether under the FCPCA or the FBCA. As the need for interoperability and trusted electronic services has grown, the FCPCA has lowered the barriers for Federal agencies to implement PKI and meet Office of Management and Budget (OMB) reporting standards. The next article in this series will focus on the SHA1FRCA.

Microsoft CA Agreement Updates

Microsoft maintains a Trust Store of CA root certificates that is distributed with every version of Microsoft Windows. To be distributed with the Trust Store, CAs must comply with requirements in the Microsoft Trust Store CA agreement. The FCPCA is just one of the certificates distributed in the Microsoft Trust Store to both increase the efficiency of the FPKI and provide interoperability with external business partners. Microsoft recently updated their CA agreement with six new requirements that address the separation of SSL and code signing from other uses of a root certificate. The FPKI Policy Authority (FPKIPA) is the governance body that rules on changes to the FCPCA; their findings could impact distribution of FCPCA certificates if compliance issues are identified. Microsoft's six new requirements and commentary on each are as follows:

1. Root certificates for code signing must use RSA 4096 or Elliptical Curve Cryptography (ECC) P384 by 2030
   FCPCA currently uses RSA 2048 but will be rekeyed by the Microsoft deadline of 2030.
2. Combination root certificates of code signing and other uses will be removed ten years from date of distribution.
   This is a best practice to mitigate the threat of a user signing malicious code with a certificate not intended for code signing. If changes are not implemented, the FCPCA will be removed from the Microsoft Trust Store in 2020. This also coincides with the timeframe for a rekey of the FCPCA. One suggestion from the FPKI community is to establish a new CA for code signing.
3. Intermediate CAs cannot issue both SSL and code signing certificates
   Usage should be limited for only those purposes intended. FCPCA does not have this restriction and changes may need to be implemented to maintain distribution.
4. New root certificates must use an Extended Key Usage (EKU) bit to separate intermediate CAs
   FPKI prohibits any use of the EKU extension on CA certificates because it violates RFC 5280. Usage of the EKU extension has been discussed extensively at the FPKI Technical Working Group (TWG) meeting on the draft FPKI Certificate Profile update and a plan for formal testing being developed. Ultimately, the decision to use EKU will be made by the FPKIPA.
5. Online Certificate Status Protocol (OCSP) is required for all end-entity certificates
   This is only required for PIV and PIV-I and is optional for other policy types.
6. Certificate serial numbers must include at least eight bytes of entropy
   FPKMA believes use of SHA2 signature should negate this requirement.

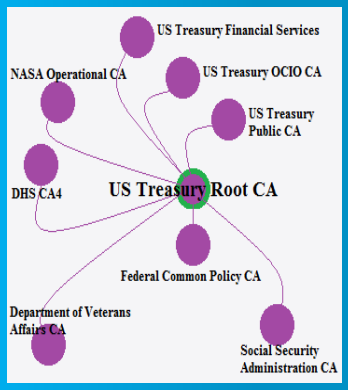
The updated CA agreement can be found at:
http://social.technet.microsoft.com/wiki/contents/articles/1760.windows-root-certificate-program-technical-requirements-version-2-0.aspx



The above image is a graphic representation of directly certified Affiliates with the FCPCA from the FPKI AIA Web Crawler. Dual lines indicate a two-way cross-certificate.

A list of the Affiliates directly certified by the FCPCA courtesy of the FPKI AIA Web Crawler can be found at:
http://fpki-graph.fpki-lab.gov

If you think your computer is hacked or in the process of being attacked, the safest action to take is to unplug the cable or conduct a hard shutdown (hold down the power button) on battery powered devices. This ensures the current state is maintained for forensic analysis.



Treasury and Entrust are just two of the SSPs certified under the FCPCA. See who else is certified at the FPKI AIA Web Crawler. http://fpki-graph.fpki-lab.gov

Industry Update: SHA1 Deprecation

Secure Hash Algorithm 1 (SHA1) is a cryptographic hash algorithm designed by the National Security Agency (NSA) in 1995. A hash algorithm can be used to uniquely identify a digital file or message to ensure data integrity (which is very important when conducting digital transactions) or it can also be used to encrypt a message. In the example below, the message "hello" was hashed using SHA1. If someone was to alter the message to "Hello" with a capital "H", the sender or receiver could distinguish the difference based on the SHA1 digest. Even a small change, such as a capital letter, can completely change the digest of the input.

Message: hello - SHA1 Digest: aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d

Message: Hello - SHA1 Digest: f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

If the original message is not known, it is near impossible to guess what it is based on the digest. Over time, algorithms that were once secure have become subject to the ever increasing speed and power of modern computers and brute force collision techniques to decrypt the messages. Similar to upgrading information systems to more powerful processors and increased memory, transitioning to more secure cryptographic algorithms should also be investigated and tested.

In 2006, NIST updated its policy on hash functions to stop using SHA1 for generating signatures, generating time stamps, and for other applications because sufficient testing demonstrated the possible compromise of SHA1. NIST advised Federal agencies to deprecate the use of SHA1 and start using SHA2 for all new applications and protocols by 2010. The commercial industry has not followed the same timeline due to the extensive use of SHA1 certificates, but has recently published guidance on a deprecated schedule phasing out usage by 2017.

Example of a website signed with an untrusted certificate

A major impact to the Federal government occurred when Microsoft published a security advisory on November 12, 2013 requesting CAs to stop issuing new SHA1 certificates; the advisory also stated that Internet Explorer will mark SHA1 certificates as untrusted after January 1, 2017. The FPKIMA successfully transitioned the FPKI Trust Infrastructure to SHA2 in 2011, but not all certified entities in the FPKI have completed the transition.

The best course of action to ensure continuity of your agency's operations is to review your certificate inventories and confirm all certificate signature algorithms and signature hash algorithms using SHA1 are scheduled to be re-issued using SHA2 or another recommended hash algorithm (i.e. Elliptical Curve Cryptography (ECC)) before January 1, 2017. After SHA1 certificates are identified and replaced, conduct a final analysis to confirm all SHA1 certificates have been replaced. This is one course of action to safeguard against any operational disruptions.

FPKI Technical Working Group

The FPKI Technical Working Group (TWG) held two meetings to discuss proposed changes to the FPKI Certificate Profiles. The FPKIMA is leading the revision of the certificate profiles to meet new Federal and industry standards and requirements.

1. A number of changes were introduced to comply with the new release of NIST Federal Information Processing Standard (FIPS) 201-2.
2. Consensus was reached on the following topics for formal recommendation to the Certificate Policy Working Group (CPWG):
    a. Combining FPKI Certificate Profiles into one document
    b. Align Signature and Public Key Algorithms/Sizes
    c. Separate Cross-Certificate vs Subordinate/Intermediate Certificate Profiles
    d. Possibly issuing new Certificate Profiles for end-user certificates
3. Items under review include making the digital signature Key Usage (KU) bit optional and making Extended Key Usage (EKU) explicit on end-entity certificates.

If you would like more information or to be added in the TWG listserv, send an email to help@fpki.gov.

Ask the FPKIMA

Why do some Affiliates issue a certificate to the FPKI?

Some affiliates issue a certificate to the FPKI because they operate an independent PKI environment with their own CP and want to use their organization's trust anchor or root certificate and certificate policies. This process is most often referred to as a cross certificate because a certificate is issued between two CAs to enable trust, interoperability, and improve business processes. This operational model is known as a non-hierarchical or bridge PKI and is used by the FBCA when there are two PKI environments that are not subordinate to each other, but business drivers exist for the users of one PKI to trust credentials issued under the other. Each CA operates under its own CP and the CPs are mapped to each other to ensure polices at a certain assurance level are equivalent. Each organization uses the policies defined in their CP and by mapping the policies across organizations, trust is created to safeguard against using a lower assurance credential at a high assurance level transaction. Without a cross certificate, the certificates from one organization in a bridge PKI would not be trusted because the path cannot be sufficiently traced to a trusted source.

Who are the FPKI SSPs and how do I contact them?

Certified FPKI SSPs are listed (with contact information) at:
http://www.idmanagement.gov/list-certified-shared-service-providers

Federal PKI Management Authority
Enabling Trust

Need Help?

Contact the FPKI Help Desk

help@fpki.gov

Cloud services such as Google Drive and Apple iCloud can be an easy and convenient way to share and store files, but they can also introduce a considerable amount of risk to the information stored there. Before using a cloud service, understand their access policies and always use two factor authentication if offered. Do the proper due diligence before using a cloud service and don't assume your personal information is safe and private.